Council of the European Union

**Brussels, 10 May 2017**
**(OR. en)**

**8579/17**

**Interinstitutional File:**
**2016/0357 (COD)**

**LIMITE**

**FRONT 184**
**VISA 147**
**DAPIX 158**
**DATAPROTECT 80**
**CODEC 665**
**COMIX 302**

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Working Party on Frontiers/Mixed Committee (EU-Iceland/Liechtenstein/Norway/Switzerland) |
| Subject: | Proposal for a Regulation of the European Parliament and of the Council establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 and (EU) 2016/1624 |

Delegations will find in the annex to this note compromise text proposals submitted by the Presidency on the recitals of the ETIAS proposal.

The text of several recitals was already in the footnotes in ST 8247/17. They have been included in the annex accordingly (recitals 12, 19a, 30, 31a, 32b, 32c and 54).

New changes are highlighted in **bold underline** and ~~double strikethrough~~ in relation to ST 14082/16.

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty of the Functioning of the European Union, and in particular, Article 77(2)(b) and (d) **and** Article 87(2)(a) ~~and Article 88(2)(a)~~ thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

After consulting the European Data Protection Supervisor,

Having regard to the opinion of the European Economic and Social Committee[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Communication of the Commission of 6 April 2016 entitled 'Stronger and Smarter Information Systems for Borders and Security'[3] outlined the need for the EU to strengthen and improve its IT systems, data architecture and information exchange in the area of border management, law enforcement and counter-terrorism. It emphasises the need to improve the interoperability of information systems. Importantly, it sets out possible options for maximising the benefits of existing information systems and, if necessary, developing new and complementary ones to address still existing information gaps.

---

1 OJ C , , p. .
2 OJ C , , p. .
3 COM(2016) 205 final.

(2) Indeed, the Communication of 6 April 2016 identified a series of information gaps. Amongst them the fact that border authorities at external Schengen borders have no information on travellers exempt from the requirement of being in possession of a visa when crossing the external borders **('the visa requirement')**. The Communication of 6 April 2016 announced that the Commission would launch a study on the feasibility of establishing a European Travel Information and Authorisation System (ETIAS)**, which was completed in November 2016**. Such an automated system would determine the eligibility of visa-exempt third country nationals prior to their travel to the Schengen Area, and whether such travel poses a security**,** ~~or irregular~~ **illegal im**migration **or public health** risk.

(3) The Communication of 14 September 2016 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders'[4] confirms the priority of securing external borders and presents concrete initiatives to accelerate and broaden the EU response in continuing to strengthen the management of external borders.

(4) It is necessary to specify the objectives of the ~~European Travel Information and Authorisation System (~~ETIAS~~)~~, to define its technical architecture, to set up the ETIAS Central Unit, the ETIAS National Units and the ETIAS Screening Board, to lay down rules concerning the operation and the use of the data to be entered into the system by the applicant, to establish rules on the issuing or refusal of the travel authorisations, to lay down the purposes for which the data are to be processed, to identify the authorities authorised to access the data and to ensure protection of personal data.

(5) The ETIAS should apply to third country nationals who are exempt from the **visa** requirement ~~of being in possession of a visa when crossing the external borders~~ **and to those who are exempt from the airport transit visa requirement**.

[4] COM(2016) 602 final.

(6) It should also apply to third country nationals who are exempt from the visa requirement who are family members of a Union citizen to whom Directive 2004/38/EC[5] applies or of a national of a third country enjoying the right of free movement **equivalent to to that of Union citizens under an agreement between the Union and its Member States on the one hand and a third country on the other** ~~under Union law~~ and who do not hold a residence card referred to under Directive 2004/38/EC **or a residence permit pursuant to Regulation (EC) No 1030/2002**. Article 21(1) of the Treaty on the Functioning of the European Union stipulates that every citizen of the Union shall have the right to move and reside freely within the territory of the Member States, subject to the limitations and conditions laid down in the Treaties and by the measures adopted to give them effect. The respective limitations and conditions are to be found in Directive 2004/38/EC on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States.

(7) As confirmed by the Court of Justice of the European Union[6], such family members have the right to enter the territory of the Member State**s** and to obtain an entry visa for that purpose. Consequently, also family members exempted from the visa obligation should have the right to obtain a travel authorisation. Member States should grant such persons every facility to obtain the necessary travel authorisation which must be issued free of charge.

---

**5** Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC.

**6** Judgment of the Court of 31 January 2006 in case C-503/03 Commission v Spain (Rec. 2006, p. I-1097).

(8) The right to obtain a travel authorisation is not unconditional as it can be denied to those family members who represent a risk to public policy, public security or public health pursuant to Directive 2004/38/EC. Against this background, family members can be required to provide their personal data related to their identification and their status only insofar these are relevant for assessment of the security threat they could represent. Similarly, examination of their travel authorisation applications should be made exclusively against the security concerns, and not those related to **im**migration risks.

(9) The ETIAS should establish a travel authorisation for third country nationals exempt from the **visa** requirement ~~to be in possession of a visa when crossing the external borders ('the visa requirement')~~ **and for those who are exempt from the airport transit visa requirement,** enabling to determine whether their presence in the territory of the Member States does not pose a~~n~~ **security,** ~~irregular~~ **illegal im**migration~~, security~~ or public health risk. Holding a valid travel authorisation should be a new entry condition for the territory of the Member States, however mere possession of a travel authorisation should not confer an automatic right of entry.

(10) The ETIAS should contribute to a high level of security, to the prevention of ~~irregular~~ **illegal im**migration and to the protection of public health by providing an assessment of visitors prior to their arrival at the external borders crossing points.

(11) ETIAS should contribute to the facilitation of border checks performed by border guards at the external border~~s~~ crossing points and ensure a coordinated and harmonised assessment of third country nationals subject to the travel authorisation requirement **who intend to travel to the Member States** ~~intending at visiting the Schengen area.~~ In addition it should enable to better inform applicants of their eligibility to **travel to the Member States**~~visit the Schengen area~~. Moreover, the ETIAS should also contribute to the facilitation of border checks by reducing the number of refusals of entry at the external borders.

(12) The ETIAS should also support the objectives of the Schengen Information System (SIS) related to the alerts in respect of persons wanted for arrest or for surrender or extradition purposes, on missing persons, on persons sought to assist with a judicial procedure and on persons for discreet checks**, [inquiry checks]** or specific checks. For this purpose the ETIAS should carry out an automated processing of the application files against the relevant alerts in the SIS. This processing will be carried **out** for the purpose of supporting the SIS. Accordingly, any hit resulting from this comparison should be ~~stored in the SIS~~ **notified to the SIRENE Bureau concerned. Once this information is transferred to the SIRENE bureau, it should be dealt with in accordance with the relevant legislation relating to the SIS.**

(13) The ETIAS should consist of a large-scale information system, the ETIAS Information System, ~~a central team,~~ the ETIAS Central Unit and ~~national teams,~~ the ETIAS National Units.

(14) The ETIAS Central Unit should be part of the European Border and Coast Guard Agency. The ETIAS Central Unit should be responsible for **determining the verification parameters for ensuring the completeness of the application and the coherence of the data, for** verifying**, where the automated application process has reported a hit,** ~~travel authorisations' applications rejected from the automated process in order to determine~~ whether the applicant**'s** personal data corresponds to the personal data of the person having triggered **that** ~~a~~ hit, **for launching the manual processing of the application, for launching the consultation process between the ETIAS National Units of the Member States involved,** for **establishing** the **specific risk indicators** ~~screening rules~~, and for carrying out regular audits on the processing of applications. The ETIAS Central Unit should work in 24/7 regime.

(15) Each Member State should establish an ETIAS National Unit mainly responsible for the examination and decision on whether to issue or refuse a travel authorisation. The ETIAS National Units should cooperate among themselves and with Europol for the purpose of the assessment of the applications. The ETIAS National Unit should **be provided with adequate resources for them to fulfil their tasks in accordance with the deadlines set out in this Regulation** ~~work in 24/7 regime~~.

(16) To meet its objectives, the ETIAS should provide an online application form that the applicant should fill in with declarations relating to his or her identity, travel document, residence information, contact details, education and current occupation, his or her condition of family member to EU citizens or third country nationals benefiting from free movement not holding a residence card **or a residence permit**, if the applicant is minor, ~~identity~~ **details** of the responsible person and answers to a set of background questions ~~(whether or not the applicant is subject to any disease with epidemic potential as defined by the International Health Regulations of the World Health Organisation or other infectious or contagious parasitic diseases, criminal records, presence in war zones, decision to return to borders/orders to leave territory)~~. Access to the applicants' health data should only be allowed to determine whether they represent a threat to public health.

(17) ETIAS should accept applications introduced on behalf of the applicant for situations where travellers are themselves not in a position to create an application, for whatever reason. In such cases, the application should be carried out by a third person authorised by the traveller or legally responsible for him/her provided this person's identity is included in the application form.

**(17a) Parameters for ensuring the completeness of the application and the coherence of the data should be established by the Central Unit to verify the admissibility of the application for travel authorisation. For instance, this verification should preclude the use of travel documents which will expire in less than six months, have expired or were issued more than ten years before. This verification should occur before the applicant is invited to pay the fee.**

(18) In order to finalise the application, all applicants above the age of **12** ~~18~~ should be required to pay a fee. The payment should be managed by a bank or a financial intermediary. Data required for securing the electronic payment should only be provided to the bank or financial intermediary operating the financial transaction and are not part of the ETIAS data.

(19) Most of the travel authorisations should be issued within minutes, however a reduced number could take **longer, especially** ~~up to 72 hours~~ for exceptional cases, where a request for additional information or documentation **or an invitation to an interview** is notified to the applicant ~~the procedure could last up to two weeks.~~

**(19a) The possibility for the ETIAS National Unit of the responsible Member State to invite an applicant to an interview should be envisaged for cases where it considers it necessary for the purposes of assessing the application. This should not be construed as a right of the applicant or an obligation on the ETIAS National Unit of the responsible Member State, but remains at the discretion of the latter, taking into account, inter alia, the presence or otherwise of a consulate of that Member State in the country of residence of the applicant. The communication between the ETIAS National Unit and the consulate should be organised by the Member State concerned taking into account security and data protection requirements, should that Member State decide to avail of itself of this possibility for the ETIAS National Unit to invite the applicant for an interview.**

(20) The personal data provided by the applicant should be processed by the ETIAS for the sole purposes of ~~verifying in advance the eligibility criteria laid down in Regulation (EU) 2016/399[7] and~~ assessing whether the ~~applicant is likely to irregularly migrate, whether the~~ entry of the applicant in the Union could pose a threat to security, **illegal immigration** or ~~to~~ public health in the Union.

[7] Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

(21) The assessement of such risks cannot be carried out without processing the personal data listed in recital (16). Each item of personal data in the applications should be compared with the data present in a record, file or alert registered in an information system (the Schengen Information System (SIS), the Visa Information System (VIS), the Europol data, the Interpol Stolen and Lost Travel Document database (SLTD), **[**the Entry/Exit System (EES), the Eurodac, the European Criminal Records Information System (ECRIS)**]** and/or the Interpol Travel Documents Associated with Notices database (Interpol TDAWN)) or against the ETIAS watchlist~~s~~, or against specific risk indicators. The categories of personal data that should be used for comparison should be limited to the categories of data present in the queried information systems, the ETIAS watchlist or the specific risk indicators.

(22) The comparison should take place by automated means. Whenever such comparison reveals that a correspondence (a 'hit') exists ~~with~~ **between** any of the personal data or combination thereof in the application~~s~~ and **that in** a record, file or alert in the above information systems, ~~or with~~ **the** personal data in the ETIAS watchlist, or ~~with~~ **the** risk indicators, the application should be processed manually by ~~an operator in~~ the ETIAS National Unit of the **responsible** Member State ~~of declared first entry~~. The assessment performed by the ETIAS National Unit should lead to the decision to issue or not the travel authorisation.

(23) The automated processing may result in the issuing of **an** authorisation. It is expected that the vast majority of applications will obtain a positive answer by automated means. No denial of a travel authorisation should be based only on the automated processing of personal data in the applications. For this reason, the applications for which a hit was generated should be assessed manually by ~~an operator in~~ an ETIAS National Unit.

(24) Applicants who have been refused a travel authorisation should have the right to appeal. Appeals should be conducted in the Member State that has taken the decision on the application and in accordance with the national law of that Member State.

(25) The screening rules should be used to analyse the application file by enabling a comparison between the data recorded in an application file ~~of the ETIAS Central System~~ and specific risk indicators corresponding to previously identified security, ~~irregular~~ **illegal im**migration or public health risk. The criteria used for defining the specific risk indicators should in no circumstances be based on a applicant's **sex,** race**,** ~~or~~ ethnic origin, ~~political opinions,~~ religion or ~~philosophical~~ belief~~s~~, ~~trade union membership, sexual life~~ **disability, age** or sexual orientation.

(26) An ETIAS watchlist should be established for identifying connections between data in an ~~ETIAS~~ application file and information related to persons who are suspected of having committed **or having taken part in a** ~~an act of~~ serious **criminal offence** ~~crime~~ or **a** terrorist~~m~~ **offence**, or regarding whom there are factual indications or reasonable grounds to believe that they will commit ~~an act of~~ serious ~~crime~~ **criminal offences or a** terrorist~~m~~ **offence**. The ETIAS watchlist should be part of the data processed by Europol in accordance with Article 18(2)(a) of Regulation (EU) 2016/794 and Europol's Integrated Data Management Concept implementing that Regulation. When providing information to Europol, Member States should be able to determine the purpose or purposes for which it is to be processed, including the possibility to limit this processing to the ETIAS watchlist.

(27) The continuous emergence of new forms of security threats, new patterns of ~~irregular~~ **illegal im**migration and public health threats requires effective responses and needs to be countered with modern means. Since these means entail the processing of important amounts of personal data, appropriate safeguards should be introduced to keep the interference with the right to protection of private life and to the right of protection of personal data limited to what is necessary in a democratic society.

(28) Personal data in ETIAS should therefore be kept secure; access to it should be limited to strictly authorised personnel and in no circumstance ~~it~~ should **it** be used to reach decisions based on any form of discrimination. The personal data stored should be kept securely in eu-LISA's facilities in the Union.

(29) Issued travel authorisations should be annulled or revoked as soon as it becomes evident that the conditions for issuing ~~it~~ **them** were not or are no longer met. In particular, when a new SIS alert is created for a refusal of entry or for a reported lost**,** ~~or~~ stolen **or invalidated** travel document, the SIS should inform the ETIAS which should verify whether this new alert corresponds to a valid travel authorisation. In such a case, the ETIAS National Unit of the **responsible** Member State ~~having created the alert~~ should be immediately informed and revoke the travel authorisation. Following a similar approach, new elements introduced in the ETIAS watchlist ~~shall~~ **should** be compared with the application files stored in the ETIAS in order to verify whether this new element corresponds to a valid travel authorisation. In such a case, the ETIAS National Unit of the **responsible** Member State ~~of first entry~~ should assess the hit and, where necessary, revoke the travel authorisation. **Similarly, a refusal of entry on certain grounds in the Entry/Exit System should trigger a reassessment, and where necessary, the revocation of the travel authorisation.** A possibility to revoke the travel authorisation at the request of the applicant should also be provided.

(30) When, in exceptional cirmcumstances, a Member State considers **it** necessary to allow a third country national to travel to its territory on humanitarian grounds, for reasons of national interest or because of international obligations, it should have the possibility to issue a travel authorisation with limited territorial and temporal validity. **Considering the nature of the travel authorisation as an authorisation to travel to the territory of Member States for the purpose of a short stay or airport transit, reasons relating to international protection do not constitute humanitarian grounds in terms of issuance of travel authorisations with limited territorial validity. With regard to international obligations, this should include the obligations deriving from the EU Charter of Fundamental Rights and should in particular cover the cases referring to the right to a fair trial.**

(31) Prior to boarding, air and sea carriers, as well as **international** carriers transporting groups overland by coach should have the obligation to verify if travellers have ~~all~~ the travel documents required for entering the territory of the Member States pursuant to the Schengen Convention[8]. ~~This should include~~ **Such carriers should** verify~~ing~~ that travellers are in possession of a valid travel authorisation. The ETIAS file itself should not be accessible to carriers. ~~A~~ Secure ~~internet~~ access **to a carrier gateway**, including the possibility **to use** ~~using~~ mobile technical solutions, should allow carriers to proceed with this consultation using travel document data.

**(31a) In establishing the technical specifications for accessing the carrier gateway, the impact on passenger travel and carriers should be limited to the extent possible. For this purpose, the relevant integration with the Entry/Exit System should be considered.**

(32) In order to comply with the revised conditions for entry, border guards should check whether the traveller is in possession of a valid travel authorisation. Therefore, during the standard border control process, the border guard should electronically read the travel document data. This operation should trigger a query to different databases as provided under the Schengen Border Code including a query to ETIAS which should provide the up-to-date travel authorisation status. The **full** ETIAS file ~~itself~~ should not be accessible to the border guard for border controls, **but certain data should be accessible to the border guards with a view to assisting them in carrying out their tasks**. If there is no valid travel authorisation, the border guard should refuse entry and should complete the border control process accordingly. If there is a valid travel authorisation, the decision to authorise or refuse entry should be taken by the border guard.

**(32a) Where the ETIAS National Unit of the responsible Member State considers that some elements of the application for a travel authorisation deserve further examination by the border guards, it may attach a flag to the travel authorisation it issues, recommending further or specific checks at the border crossing point.**

---

[8] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders.

**(32b) The address for the first intended stay declared in the application being different from the address declared at entry should not lead to an automatic refusal of entry at the border by the border guards.**

**(32c) Since the possession of a valid travel authorisation is a condition of entry and stay for certain categories of third country nationals, the immigration authorities of the Member States should be able to consult the ETIAS Central System. Immigration authorities of the Member States should have access to certain information stored in the ETIAS Central System, in particular for the purpose of returns. They should search the ETIAS Central System using the information which is contained in the machine readable zone of a travel document without necessarily using specific equipment for that purpose.**

(33) In the fight against terrorist offences and other serious criminal offences and given the globalisation of criminal networks, it is imperative that ~~law enforcement~~ **designated** authorities **responsible for the prevention, detection or investigation of terrorist offences and other serious criminal offences ('designated authorities')** have the necessary information to perform their tasks effectively. Access to data contained in the Visa Information System (VIS) for l~~aw enforcement~~ **such** purpose has already proven effective in helping investigators to make substantial progress in cases related to human being trafficking, terrorism or drug trafficking. The Visa Information System does not contain data on visa-exempt third-country nationals.

(34) Access to the information contained in ETIAS is necessary to prevent, detect and investigate terrorist offences as referred to in **Directive 2017/541(EU)** ~~Council Framework Decision 2002/475/JHA~~[9] or other serious criminal offences as referred to in Council Framework Decision 2002/584/JHA[10]. In a specific investigation and in order to establish evidence and information related to a person suspected of having committed a **serious** crime or a victim of a **serious** crime, ~~law enforcement~~ **designated** authorities may need access to the data generated by ETIAS. The data stored in ETIAS may also be necessary to identify the perpetrator of a terrorist offence or other serious criminal offences, especially when urgent action is needed. Access to the ETIAS for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences constitutes an interference with the fundamental rights to respect for the private life of individuals and to protection of personal data of persons whose personal data are processed in the ETIAS. Therefore, the data in ETIAS should be retained and made available to the designated authorities of the Member States and the European Police Office ('Europol'), subject to the strict conditions set out in this Regulation in order for such access to be limited to what is strictly necessary for the prevention, detection and investigation of terrorist offences and **other** serious criminal offences in accordance with the requirements notably laid down in the jurisprudence of the Court, in particular in the Digital Rights Ireland case[11].

---

[9] **Directive (EU) 2017/541 of 15 March 2017 on combatting terrorism and replacing** Council Framework Decision 2002/475/JHA **and amending Council Directive 2005/671/JHA (OJ L 88, 31.03.2017, p. 6)** ~~of 13 June 2002 on combatting terrorism (OJ L 164, 22.6.2002 p.6)~~.

[10] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member State (OJ L 190, 18.7.2002, p. 1).

[11] Judgment of the Court (Grand Chamber) of 8 April 2014 in joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd, ECLI:EU:C:2014:238.

(35) In particular, access to ETIAS data for the purpose of preventing, detecting or investigating terrorist offences or other serious criminal offences should only be granted following a reasoned request by the **operating unit of the designated authoritiy** ~~competent authorities~~ giving reasons for its necessity. ~~Member States should ensure that any such request for access to data stored in ETIAS be the subject of a prior review by a court or by an authority providing guarantees of full independence and impartiality, and which is free from any direct or indirect external influence. However, in situations of extreme urgency, it can be crucial for the competent authorities~~ **Where there is a need** to **immediately** obtain ~~immediately~~ personal data necessary for preventing ~~the commission~~ **a terrorist offence or an imminent danger associated with another** ~~of a~~ serious **criminal offence** ~~crime~~ or so that its perpetrators can be prosecuted, ~~In such cases~~ it should be accepted that the **verification as to whether the conditions were fulfilled** ~~review of the personal data obtained from ETIAS~~ takes place as swiftly as possible after access to such data has been granted to the **designated** ~~competent~~ authorities.

(36) It is therefore necessary to designate the ~~competent~~ authorities of the Member States that are authorised to request such access for the specific purposes for the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

(37) ~~The ETIAS National Units should act as~~ The central access point**(s)** **designated by each Member State** ~~and~~ should verify that the conditions to request access to the ETIAS Central System are fulfilled in the concrete case at hand.

(38) Europol is the hub for information exchange in the Union and it plays a key role with respect to cooperation between Member States' authorities in the field of cross-border crime investigation in supporting Union-wide crime prevention, analyses and investigation. Consequently, Europol should also have access to the ETIAS Central System within the framework of its tasks and in accordance with Regulation (EU) 2016/794[12] in specific cases where this is necessary for Europol to support and strengthen action by Member States in preventing, detecting or investigating terrorist offences or other serious criminal offences.

[12] OJ L 119, 4.5.2016, p. 132-149.

(39) To exclude systematic searches, the processing of data stored in the ETIAS Central System should take place only in specific cases and only when it is necessary for the purposes of preventing, detecting or investigating terrorist offences or other serious criminal offences. The designated authorities and Europol should only request access to ETIAS when they have reasonable grounds to believe that such access will provide information that will substantially assist them in preventing, detecting or investigating a terrorist offence or other serious criminal offence. ~~The law enforcement authorities and Europol should only request access to the ETIAS if prior searches in all relevant national databases of the Member State and databases at Europol did not lead to the requested information.~~

(40) The personal data recorded in the ETIAS should be kept for no longer than is necessary for its purposes. In order for the ETIAS to function, it is necessary to keep the data related to applicants for the period of validity of the travel authorisation. In order to assess the security, ~~irregular~~ **illegal im**migration and public health risks posed by the applicants it is necessary to keep the personal data for five years from the last entry**/exit** record of the applicant stored in the EES. In fact, the ETIAS should rely on accurate preliminary assessments of the security, ~~public health and~~ ~~irregular~~ **illegal im**migration **and public health** risks, notably through the use of the screening rules. In order to constitute a reliable basis for the manual risk assessment by the Member States, and reduce to the minimum the occurrence of hits not corresponding to real risks ('false positives'), the hits resulting from screening rules based on statistics generated by ETIAS data itself need to be representative of a sufficiently broad population. This cannot be achieved exclusively on the basis of the data of the travel authorisations in their validity period. The retention period should start from the last entry**/exit** record of the applicant stored in the EES, since that constitutes the last actual use of the travel authorisation. A retention period of five years corresponds to the retention period of an ~~EES~~ **entry/exit** record with an entry authorisation granted on the basis of an ETIAS travel authorisation or a refusal of entry. This synchronisation of retention periods ensures that both the entry**/exit** record and the related travel authorisation are kept for the same duration and is an additional element ensuring the future interoperability between ETIAS and EES. This synchronisation of data retention periods is necessary to allow the competent authorities to perform the risk analysis requested by the Schengen

Borders Code. A decision to refuse, revoke or annul a travel authorisation could indicate a higher security**,** ~~or irregular~~ **illegal im**migration **or public health** risk posed by the applicant. Where such a decision has been issued, the 5 years retention period for the related data should start from ~~its~~ **the** date of **that decision**~~issuance~~, in order for ETIAS to be able to take accurately into account the higher risk possibly posed by the applicant concerned. After the expiry of such period, the personal data should be deleted.

(41) Precise rules should be laid down as regards the responsibilities of the Agency for the operational management of large-scale information systems in the area of freedom, security and justice (eu-LISA) for the design~~ing~~, development and technical management of the ETIAS Information System, the respons~~a~~**i**bilities of the European ~~Coast and~~ Border **and Coast** Guard Agency, the responsibilities of the Member States and the respons~~a~~**i**bilities of Europol.

(42) Regulation (EC) No 45/2001 of the European Parliament and the Council[13] applies to the activities of eu-LISA and the European ~~Coast and~~ Border **and Coast** Guard Agency when carrying out the tasks entrusted to them in this Regulation.

(43) [Regulation (EU) 2016/679][14] applies to the processing of personal data by the Member States' **authorities** in application of this Regulation unless such processing is carried out by the designated ~~or verifying~~ authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences.

---

**13** Regulation (EC) No 45/2001 of the European Parliament and the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1).

**14** Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

(44) **[Directive (EU) 2016/680]**[15] **applies to** the processing of personal data by the **designated** authorities of the Member States for the purposes of the prevention, detection or investigation of terrorist offences or of other serious criminal offences pursuant to this Regulation ~~should be subject to a standard of protection of personal data under their national law which complies with [Directive (EU) 2016/680]~~.

(45) The independent supervisory authorities established in accordance with [Regulation (EU) 2016/679] should monitor the lawfulness of the processing of personal data by the Member States, whilst the European Data Protection Supervisor as established by Regulation (EC) No 45/2001 should monitor the activities of the Union institutions and bodies in relation to the processing of personal data. The European Data Protection Supervisor and the supervisory authorities should cooperate with each other in the monitoring of the ETIAS.

(46) The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 and delivered an opinion on **6 March 2017**.

(47) Strict access rules to the ETIAS Central System and the necessary safeguards should be established. It is also necessary to provide for individuals' rights of access, correction, deletion and redress, in particular the right to a judicial remedy and the supervision of processing operations by public independent authorities.

---

**15** Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

(48) In order to assess the security, ~~irregular~~ **illegal im**migration or public health risk which could be posed by a traveller, interoperability between the ETIAS Information System and other **EU** information systems ~~consulted by ETIAS such as the Entry/Exit System (EES), the Visa Information System (VIS), the Europol data, the Schengen Information System (SIS), the Eurodac and the European Criminal Records Information System (ECRIS)~~ should ~~have to~~ be established **for the purpose of implementing this Regulation**. ~~However this interoperability can only be fully ensured once the proposals to establish the EES[16], the ECRIS[17] and the recast proposal of the Eurodac Regulation[18] have been adopted~~.

(49) ~~The effective monitoring of the application of this Regulation requires evaluation at regular intervals. The Member States should lay down rules on the penalties applicable to infringements of the provisions of this Regulation and ensure that they are implemented.~~ **Member States should take the necessary measures to ensure that the penalties applicable to infringements of the provisions of this Regulation are dissuasive, effective and proportionate and that they are implemented.**

(50) In order to establish the technical measures needed for the application of this Regulation, the power to adopt acts in accordance with Article 290 of the Treaty on the Functioning of the European Union should be delegated to the Commission:

---

**16** Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Union and determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No 767/2008 and Regulation (EU) COM(2016) 194 final.

**17** Proposal for a Directive of the European Parliament and of the Council amending Council Framework Decision 2009/315/JHA, as regards the exchange of information on third country nationals and as regards the European Criminal Records Information System (ECRIS), and replacing Council Decision 2009/316/JHA.

**18** Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person] , for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) COM(2016) 272 final.

– to adopt a predetermined list of answers concerning the questions on the level and field of education, the current occupation and the job title to be indicated in the application for a travel authorisation,

– **to specify the content and format of questions relating to diseases, convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions which can be put to an applicant for a travel authorisation,**

– to specify the content and format of ~~the~~ additional questions ~~which can be put~~ to ~~an~~ **the** applicant **having replied affirmatively to one of the questions relating to diseases, convictions for criminal offences, stays in war or conflict zones and decisions to leave the territory or return decisions,**~~for a travel authorisation~~,

– to lay down the payment methods and process for the travel authorisation fee **and the changes to the amount of that fee** taking into account **any increase in the costs of the ETIAS** ~~the technological developments and their availability and to amend the amount of the fee~~,

– **to lay down the content and format of a predetermined list of options when the applicant is requested to provide additional information or documentation,**

– to **regularly identify specific risks relating to** ~~further specify~~ ~~the~~ security, ~~irregular~~ **illegal im**migration or public health ~~risks~~ to be used for the establishment of the risk indicators **in order to ensure adaptation in view of the continuous emergence of new risks and patterns**,

– to extend the duration of the **transitional** period ~~of grace~~ during which no travel authorisations is required, **as well as of** ~~to extend~~ the duration of the period of grace during which ~~no~~ **a** travel authorisations is required **but in which border guards will allow third country nationals not in possession of the travel authorisation exceptionally to enter subject to certain conditions.**

~~– to further specify the security, irregular migration or public health risks to be used for the establishment of the risk indicators.~~

(51) It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level, and that those consultations be conducted in accordance with the principles laid down in the Interinstitutional Agreement on Better Law-Making of 13 April 2016. In particular, to ensure equal participation in the preparation of delegated acts, the European Parliament and the Council receive all documents at the same time as Member States' experts, and their experts systematically have access to meetings of Commission expert groups dealing with the preparation of delegated acts.

(52) In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission to adopt detailed rules on the conditions for operation of the public website and the mobile app for mobile devices and on the data protection and security rules applicable to the public website and the mobile app for mobile devices, **to establish the technical specifications of the ETIAS watchlist, to adopt** ~~as well as~~ an authentication scheme reserved exclusively to carriers and to specify the details of the fall-back procedures to be followed in the case of technical impossibility to access **data by carriers** ~~ETIAS~~**, to adopt model contingency plans in case of technical impossibility to access data at the external borders or failure of the ETIAS, to adopt a model security plan and a model business continuity and disaster recovery plan in relation to security of processing of personal data, to lay down and develop a mechanism, procedures and interpretation of data quality compliance, to draw up a common leaflet to inform travellers, to adopt detailed rules on the operation of the central repository and the data protection and security rules applicable to the repository, and to make available to Member States a technical solution in order to facilitate the collection of certain data**. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council[19].

[19] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commision's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13).

(53) The establishment of ~~a~~ ETIAS and the creation of common obligations, conditions and procedures for use of data cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale and impact of the action, be better achieved at Union level in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality, as set out in that Article, the Regulation does not go beyond what is necessary in order to achieve this objective.

(54) ~~The projected costs for the development of the ETIAS Information System and for the establishment of the ETIAS Central Unit and the ETIAS National Units are lower than the remaining amount on the budget earmarked for Smart Borders in Regulation (EU) No 515/2014 of the European Parliament and the Council[20]. Accordingly, this Regulation, pursuant to Article 5(5)(b) of Regulation (EU) No 515/2014, should, re-allocate the amount currently attributed for developing IT systems supporting the management of migration flows across the external borders.~~ **The operational and maintenance costs of the ETIAS Information System, the ETIAS Central Unit and of the ETIAS National Units should be covered entirely by the revenues generated by the fees. The fee should therefore be adapted as necessary, having regard to the costs.**

[(55) The revenue generated by the payment of travel authorisation fees should be assigned to cover the recurring operational and maintenance costs of the ETIAS Information System, of the ETIAS Central Unit and of the ETIAS National Units. In view of the specific character of the system, it is appropriate to treat the revenue as external assigned revenue.]

---

**20** Regulation (EU) No 515/2014 of the European Parliament and of the Council of 16 April 2014 establishing as part of the Internal Security Fund, the Instrument for financial support for external borders and visa and repealing Decision No 574/2007/EC (OJ L 150, 20.5.2014, p. 143).

(56) This Regulation is without prejudice to the application of Directive 2004/38/EC.

(57) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark is not taking part in the adoption of this Regulation and is not bound by it or subject to its application. Given that this Regulation builds upon the Schengen *acquis*, Denmark shall, in accordance with Article 4 of that Protocol, decide within a period of six months after the Council has decided on this Regulation whether it will implement it in its national law.

(58) This Regulation constitutes a development of the provisions of the Schengen acquis in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC[21]; the United Kingdom is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

(59) This Regulation constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC[22]; Ireland is therefore not taking part in the adoption of this Regulation and is not bound by it or subject to its application.

---

[21] Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen acquis (OJ L 131, 1.6.2000, p. 43).

[22] Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen acquis (OJ L 64, 7.3.2002, p. 20).

(60) As regards Iceland and Norway, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latters' association with the implementation, application and development of the Schengen acquis[23] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC[24].

(61) As regards Switzerland, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[25] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2008/146/EC[26] and with Article 3 of Council Decision 2008/149/JHA[27].

---

23 OJ L 176, 10.7.1999, p. 36.

24 Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen acquis (OJ L 176, 10.7.1999, p. 31).

25 OJ L 53, 27.2.2008, p. 52.

26 Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis (OJ L 53, 27.2.2008, p. 1).

27 Council Decision 2008/149/JHA of 28 January 2008 on the conclusion on behalf of the European Union of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation’s association with the implementation, application and development of the Schengen acquis (OJ L 53, 27.2.2008, p. 50).

(62) As regards Liechtenstein, this Regulation constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*[28] which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU[29] and with Article 3 of Council Decision 2011/349/EU.[30]

~~(63) This Regulation constitutes an act building upon, or otherwise relating to, the Schengen *acquis* within, respectively, the meaning of Article 3(2) of the 2003 Act of Accession, Article 4(2) of the 2005 Act of Accession and Article 4(2) of the 2011 Act of Accession.~~

(64) In order to have this Regulation fit into the existing legal framework and reflect the changes for the European **Border and** Coast ~~and Border~~ Guard Agency ~~and Europol the~~ Regulations (EU) No 515/2014, (EU) 2016/399~~, (EU) 2016/794~~ and (EU) 2016/1624 should be amended accordingly.

---

**28** OJ L 160, 18.6.2011, p. 21.

**29** Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

**30** Council Decision 2011/349/EU of 7 March 2011 on the conclusion on behalf of the European Union of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen acquis relating in particular to judicial cooperation in criminal matters and police cooperation (OJ L 160, 18.6.2011, p. 1).